

**UNITED STATES DEPARTMENT OF COMMERCE****U.S. Patent and Trademark Office**

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
09783146	2/13/01	VANHEYNINGEN ET AL.	05313.00003

Banner & Witcoff, Ltd.
1001 G. Street, N.W.
Washington, DC 20001-4597

EXAMINER

Christopher J. Brown

ART UNIT	PAPER
----------	-------

2134

20070611

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Examiner Brown conversed with Brad Wright about application 09783146 on 7/23/07. Examiner Brown assured Mr. Wright that the application had been allowed, and would not be abandoned on 7/24/07. Mr Wright requested a statement on the record for the purposes of appeal or a need for petition to revive.

CJB

Notice of Allowability

Application No.

09/783,146

Examiner

Christopher J. Brown

Applicant(s)

VANHEYNINGEN ET AL.

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 6/6/07.
2. ☒ The allowed claim(s) is/are 1-7, 9-20, 22-26, 28, 30-43, 45-46.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☒ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material

5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

An extension of time under 37 CFR 1.136(a) is required in order to make an examiner's amendment which places this application in condition for allowance. During a telephone conversation conducted on June 6th 2007 Applicant requested an extension of time for 4 MONTH(S) and authorized the Director to charge Deposit Account No. 19-0733 the required fee for this extension and authorized the following examiner's amendment.

Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

This listing of claims will replace all prior versions, and listings, of claims in the application.

IN THE CLAIMS:

1. (Currently Amended) A method of transmitting data securely over a computer network, comprising the steps of:

- (1) establishing a communication path between a first computer and a second computer;
- (2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record;
- (3) in the second computer, receiving and decrypting the data records transmitted in step

Art Unit: 2134

(2) without reference to a previously received data record; and

(4) in the second computer, transmitting session information for encrypting and decrypting the data records to a third computer,

wherein step (2) comprises the step of embedding an indicator in each of the data records indicating that the data records are encrypted according to an encryption scheme that encrypts records without regard to any previously transmitted data records, and

wherein step (3) comprises the step of determining whether the indicator is present in each record and, in response to determining that the indicator is not present, processing each such record differently than if the indicator is set.

2. (Original) The method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path.

3. (Original) The method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2).

4. (Original) The method of claim 2, wherein the session information includes at least a portion of the security credentials.

5. (Original) The method of claim 1, wherein step (2) comprises the step of incorporating a nonce in each data record that is used by the second computer in combination with a previously shared encryption key to decrypt each of the data records in step (3).

6. (Original) The method of claim 5, wherein the nonce comprises a random number.

7. (Original) The method of claim 5, further comprising the step of, in the second

Art Unit: 2134

computer, verifying that the nonce has not previously been received in a previously transmitted data record.

8. (canceled)

9. (Original) The method of claim 1, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol.

10. (Original) The method of claim 1, wherein step (2) is performed by a proxy server that encrypts data records received from another server.

11. (Original) The method of claim 1, wherein the third computer establishes a communication path with the first computer; and encrypts and transmits data records to the first computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record and by employing the session information.

12. (Original) The method of claim 1, wherein a fourth computer retrieves the session information from the third computer, establishes a communication path with the first computer; and encrypts and transmits data records to the first computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record and by employing the session information.

13. (Original) The method of claim 1, wherein the session information is SSL or TLS session information.

14. (Original) The method of claim 1, wherein the session information includes a SSL or

Art Unit: 2134

TLS session identifier.

15. (Original) The method of claim 1, wherein the session information includes an encryption key that is used to encrypt data records in step (2).

16. (Original) The method of claim 1, wherein the session information is stored by the third computer in a cache memory using a hash function.

17. (Original) The method of claim 16, wherein the hash function is the BUZhash function.

18. (Original) The method of claim 1, wherein the second computer transmits the session information to the third computer using multicast communication.

19. (Original) The method of claim 18, wherein the multicast communication is negative acknowledgement multicast communication.

20. (Currently Amended) A method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of:

- (1) establishing a reliable connection between the client computer and the proxy server;
- (2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection;
- (3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records;
- (4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records;

Art Unit: 2134

(5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol;

(6) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key; and

(7) in the proxy server, transmitting session information including the previously shared encryption key for use in decrypting the plurality of data records to another server,

wherein step (6) comprises the step of checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing decryption of the received data record using the corresponding nonce.

21. (Canceled)

22. (Original) The method of claim 20, wherein step (3) comprises the step of generating a random number as each nonce.

23. (Original) The method of claim 20, wherein step (3) comprises the step of generating an unique number as each nonce.

24. (Original) The method of claim 20, wherein step (1) is performed using Transmission Control Protocol, and wherein step (5) is performed using User Datagram Protocol.

25. (Original) The method of claim 20, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol.

26. (Original) The method of claim 25, wherein the reliable communication protocol is Transmission Control Protocol.

27. (canceled)

28. (Currently Amended) A method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of:

(1) establishing a reliable connection between the client computer and the proxy server;

(2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection;

(3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records;

(4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records;

(5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol;

(6) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key; and

(7) in the proxy server, transmitting session information including the previously shared encryption key for use in decrypting the plurality of data records to another server,

wherein the another server is a second proxy server, and

further including, in the second proxy server, decrypting encrypted data records from the client computer using a corresponding nonce extracted from each data record and the session

Art Unit: 2134

information transmitted from the first proxy server.

29. (Canceled)

30. (Currently Amended) A method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of:

(1) establishing a reliable connection between the client computer and the proxy server;

(2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection;

(3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records;

(4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records;

(5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol;

(6) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key; and

(7) in the proxy server, transmitting session information including the previously shared encryption key for use in decrypting the plurality of data records to another server,

wherein the another proxy server is a cache memory server, and
further including, in a second proxy server,

obtaining the session information from the cache memory server, and
decrypting encrypted data records from the client computer using a corresponding nonce
extracted from each data record and the session information.

31. (Currently Amended) The method of claim 20, wherein the session information is
SSL or TLS session information.

32. (Currently Amended) The method of claim 20, wherein the session information
includes a SSL or TLS session identifier.

33. (Original) The method of claim 20, wherein the session information includes
authentication information for a user of the client computer.

34. (Currently Amended) The method of claim 20, wherein the session information is
stored by the another server in a cache memory using a hash function.

35. (Original) The method of claim 34, wherein the hash function is the BUZhash
function.

36. (Currently Amended) The method of claim 20, wherein the proxy server transmits the
session information to the another server using multicast communication.

37. (Original) The method of claim 36, wherein the multicast communication is negative
acknowledgement multicast communication.

38. (Currently Amended) A system for securely transmitting data using an unreliable
protocol, comprising:

a first computer having a communication protocol client function operable in conjunction
with an application program to transmit data records securely using an unreliable protocol; and
a second computer coupled to the first computer and having a communication protocol

Art Unit: 2134

server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol,

wherein the communication protocol client function encrypts each data record using a nonce and an encryption key and appends the respective nonce to each of the encrypted data records; and

wherein the communication protocol server function decrypts each of the data records using the respectively appended nonce and the encryption key; and

a third computer coupled to the second computer and having a cache memory for storing at least the encryption key,

wherein the second computer comprises a record detector that determines whether an indicator has been set in each data record received from the first computer and, if the indicator has not been set for a data record, bypassing decryption of that data record by the communication protocol server function.

39. (Original) The system of claim 38, wherein the communication protocol client function exchanges encryption credentials with the communication protocol server function using a reliable communication protocol.

40. (Currently Amended) The system of claim 39, wherein the unreliable communication protocol includes the User Datagram Protocol, and wherein the reliable communication protocol includes the Transmission Control Protocol.

41. (Original) The system of claim 38, wherein the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol.

Art Unit: 2134

42. (Original) The system of claim 38, wherein the communication protocol client function and the communication protocol server function are compatible with the SSL/TLS communication protocol.

43. (Original) The system of claim 38, wherein the second computer comprises a proxy server that forwards decrypted records received from the first computer to a server computer.

44. (Canceled)

45. (Original) The system of claim 38, wherein the third computer is a proxy server that can receive encrypted records from the first computer;
can decrypt records the received records using at least the encryption key stored in the cache memory; and

can forward the decrypted records received from the first computer to a server computer.

46. (Currently Amended) A system for securely transmitting data using an unreliable protocol, comprising:

a first computer having a communication protocol client function operable in conjunction with an application program to transmit data records securely using an unreliable protocol; and

a second computer coupled to the first computer and having a communication protocol server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol,

wherein the communication protocol client function encrypts each data record using a nonce and an encryption key and appends the respective nonce to each of the encrypted data records; and

wherein the communication protocol server function decrypts each of the data

Art Unit: 2134

records using the respectively appended nonce and the encryption key; and
a third computer coupled to the second computer and having a cache memory for storing
at least the encryption key, wherein the third computer is a memory cache server, and
further including a fourth computer that can
obtain the at least the encryption key stored in the cache memory of the third
computer;
receive encrypted records from the first computer;
decrypt records the received records using at least the encryption key stored in the
cache memory; and
forward the decrypted records received from the first computer to a server
computer.

47-58 (Canceled)

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: Please see the merits on the record for explanation of allowable subject matter..

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Oath/Declaration

The Oath/Declaration submitted on 6/18/2001 is defective because the inventor Rodger Erickson has not signed the document.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

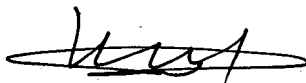
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown



6/11/07



**KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER**